Application Security: Securing your code as you develop

Application security is a set of measures designed to prevent data or code at the application level from being stolen or manipulated. It spotlights security *during* application development & design phases AND systems & approaches that protect applications *after* deployment. The right application security strategy should ensure protection across all types of applications used by any stakeholder, whether internal or external.

Inherited vulnerabilities, the need to find qualified experts for a security team, and ensuring security throughout the application development life cycle are common challenges that modern **application security** presents.

Application security tools involve different kinds of security testing for different types of applications, and there's always a right time to use each security tool.

Static Application Security Testing (SAST)

SAST is a type of application security testing that focuses on code. It works early in the CI pipeline and scans source code, bytecode, or binary code in order to identify problematic coding patterns that go against best practices. SAST is programming-language dependent.

Dynamic Application Security Testing (DAST)

DAST is a black-box testing method that scans applications in runtime. It's applied later in the CI pipeline. DAST is a good method for preventing regressions and doesn't depend on a specific programming language. DAST fits best with application security testing methods that rely on static checks, like SAST and SCA, since it provides additional runtime insights to the static source-code analysis.

Software Composition Analysis / Open Source Security & Compliance (SCA/OSS)

SCA focuses on third-party code dependencies that are used in the application. SCA is very effective in applications that use many open-source libraries. SCA is programming language-dependent.

Interactive Application Security Testing (IAST)

IAST is essentially a combination of SAST and DAST application security testing methods. IAST analyzes only the code executed in your tests, like DAST, but it also pinpoints the exact place in the code where the vulnerability was found, as with SAST.

Mobile Application Security Testing (MAST)

MAST is a type of application security testing that focuses on mobile apps. MAST combines static analysis, dynamic analysis, and penetration testing to effectively assess risk areas of the mobile app.

Runtime Application Self-Protection (RASP)

RASP acts like a net, using application data and contextual information to stop attacks that have slipped by the WAF or other preventative security tools.

Ensure cybersecurity excellence

Build a more efficient and robust cyber security ecosystem with Opticca Security, your consultative partner. With established relationships with leading cyber security vendors like Cloudflare, ShiftLeft, Snyk, and Sonatype, we can deliver solutions that pair best-in-class technology with your strategic objectives.

As you navigate the security challenges of application development, we're here to help – now and as your needs evolve.

Let's begin with a conversation.

opticcasecurity.com
opticca-security

info@opticcasecurity.com
6500 Trans-Canada Hwy
Suite 400
Pointe Claire, QC
H9R 0A5
Canada

opticca security